REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE 9/30/04	3. REPORT TYPE AND DATES COVERED Annual Report 01 Jul 02 - 31 Jan 05
4. TITLE AND SUBTITLE Secure Tactical Mobile Intelligent Agents		5. FUNDING NUMBERS DAAD 19-02-1-0235
6. AUTHOR(S) Mike Burmester and Alec Yasinsac		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Florida State University 257 James Jay Love Bldg. Tallahassee, FL 32306-4166		8. PERFORMING ORGANIZATION REPORT NUMBER 4
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U. S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211		10. SPONSORING / MONITORING AGENCY REPORT NUMBER 43588.14-CI

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT	12 b. DISTRIBUTION CODE
Approved for public release; distribution unlimited.	

13. ABSTRACT (Maximum 200 words)

Research on protocols in ad hoc networks, secret sharing to support distributed computation, and mechanisms to enhance data encapsulation for mobile computations has continued since our Interim Progress Report. Several papers were published or submitted for publication relating to the research conducted in relation to this project. An important discovery relating to the family of algorithms that can guarantee node and link disjoint paths in ad hoc networks of reasonable size and density. A message delivery mechanism that resists broadcast storm while retaining the positive reliability properties of flooding was also developed.

Work in progress

Willard Thompson has devised a framework and corresponding mechanism for protecting privacy of computations by mobile agents called "Semantic Encryption Transformation Scheme".

Additional work by non-ARO funded students

Todd MacDonald, a self-funded Ph.D. student of PI Yasinsac is also working in this area and has amassed a large volume of work in homomorphic encryption and protocol verification for mobile agent schemes.

Khandy Polite is a DoD IASP student that conducted research in an area closely related to mobile agent security. Her thesis is entitled: " Privacy Preserving Data Aggregation in Wireless Sensor Networks" was completed in April 2004.

Another DoD IASP student, Anna Suen, completed a Mobile Agent security related thesis entitled: "_Mobile Agent Protection with Data Encapsulation and Execution Tracing" in April 2003.

14. SUBJECT TERMS Mobile Agents, Wireless Security Protocols, Provable Security			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OR REPORT **UNCLASSIFIED**	18. SECURITY CLASSIFICATION ON THIS PAGE **UNCLASSIFIED**	19. SECURITY CLASSIFICATION OF ABSTRACT **UNCLASSIFIED**	20. LIMITATION OF ABSTRACT **UL**

1. List of papers

1.1. Papers published in peer-review journals NA

1.2. Papers published in non-peer-reviewed journals or in conference proceedings

1.2.1. Donald J. Scott and Alec Yasinsac, “Dynamic Probabilistic Retransmission in Ad hoc Networks”, Proceedings of the *International Conference on Wireless Networks*, June 21-4, 2004

1.2.2. Prabha Ramachandran and Alec Yasinsac, "Limitations of On Demand Secure Routing Protocols", IEEE Wireless Communications and Networking Conference 2004, September 2004

1.2.3. M. Burmester and Tri van Le, “Secure Multipath Communication in Mobile Ad hoc Networks”, Proceedings International Conference on Information Technology Coding and Computing, Las Vegas Nevada, April 5-7, 2004

1.2.4. M. Burmester and Tri van Le, “Tracing Byzantine faults in ad hoc networks”, Proceedings, Computer, Network and information Security 2003, New York, December 10 – 12, 2003

1.2.5. Mike Burmester and Alec Yasinsac “Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks” 2004 Cambridge Workshop on Selected areas on Security. 2004

1.2.6. Mike Burmester and Alec Yasinsac, "Modeling Trust in Ad hoc Networks", *6th WSEAS International Conference on Telecommunications and Informatics*, May 12-15, 2004

1.2.7. Mike Burmester and Alec Yasinsac, "Protocols for a Dynamic Key Exchange System for Ad Hoc Networks", *Eleventh International Workshop on Security Protocols*, Cambridge, UK, Apr. 2-4, 2003, Lecture Notes in Computer Science

1.2.8. Willard C. Thompson III, Alec Yasinsac, and J. Todd McDonald, "Semantic Encryption Transformation Scheme", *2004 International Workshop on Security in Parallel and Distributed Systems*, September 15-17, 2004, , pp. 516-21

1.2.9. J. Todd McDonald, Alec Yasinsac, and Willard C. Thompson III, "Mobile Agent Data Integrity Using Multi-agent Architecture", *2004 International Workshop on Security in Parallel and Distributed Systems*, September 15-17, 2004, pp.

1.2.10. Mike Burmester, Tri Le Van, and Alec Yasinsac, " Weathering the Storm: Managing Redundancy and Security in Ad hoc Networks ", *3rd International Conference on AD-HOC Networks & Wireless*, July 20-22, 2004, **Lecture Notes in Computer Science** 3158, Springer, pp. 96-107

1.2.11. M. Burmester and T. van Le. `Secure Communication in Ad hoc Networks'. Proceedings of the IEEE Workshop on Information Assurance and Security', West Point, NY, pp. 234--241, June 2004.

1.2.12. M. Burmester and T. van Le. `Secure Multipath Communication in Mobile Ad hoc Networks'. International Conference on Information Technology: Coding and Computing (ITCC 2004), Las Vegas, April 5-7, 2004

1.2.13. M. Burmester T. van Le and M. Weir. `Tracing Byzantine faults in ad hoc networks'. Communication, Network and Information Security 2003, Dec 10-12 2003, New York, pp.43-46.

1.3. Papers presented at meetings, but not published in conference proceedings NA

1.4. Manuscripts submitted, but not published

1.4.1. Tysen Leckie and Alec Yasinsac, "Metadata for Anomaly Based Security Protocol Attack Detection", To appear IEEE Transactions on Knowledge and Data Engineering, 2004

1.4.2. Alec Yasinsac, “Weathering the storm: managing redundancy and security in ad hoc networks.”, The 9th Australian Conference on Information Security and Privacy, July 13 – 15, 2004.

1.5. Technical reports submitted to ARO NA

2. List of all participating scientific personnel showing any advanced degrees earned by them while employed on the project.

2.1. Tri van Le received his Ph. D in Computer Security, in the spring semester of 2004.

3. Report of Inventions NA

4. Statement of the problem studied

The investigators have studied problems of mobile tactical communications with the goal of supporting battlefield comm. Much of the work over this reporting period has involved research of fundamental theories that support protecting the logical computing infrastructure and techniques for protecting communication applications among mobile nodes. Secure routing, mitigating broadcast storms, intrusion detection in encrypted environments, secure data aggregation, and enabling key distribution in low power, low bandwidth environments are the areas most considered.

5. Summary of the most important results

5.1. The investigators discovered a family of algorithms that can guarantee node and link disjoint paths in ad hoc networks of reasonable size and density. Properties of these algorithms make them excellent candidates for implementation in low power environments.

5.2. A second important result involves a message delivery mechanism that resists broadcast storm while retaining the positive reliability properties of flooding. This mechanism involves establishing hexagonal tiles allowing node-oriented flooding to be reduced to tile-flooding. This system reflects the strongest Byzantine security properties where if there is at least one honest member in each tile, broadcast messages are guaranteed to reach every member in the target group.

5.3. A classic problem in distributed computing is mobile code protection. One approach to solving that problem is through program obfuscation/encryption. The investigators have discovered architecture for systematically confusing code to prevent predictable-result malicious activity. The architecture also establishes a forum and mechanisms for verifying and measuring the level of confusion in the mobile modules.

5.4 The investigators defined an approach to mobile agent systems security using a multi-agent approach. My partitioning the security task into sub-components, redundant, collaborative processes can be applied to ensure and verify results of distributed data collection and computation